



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/240,265	01/29/1999	MARK E. PETERS	CR9-98-095	7166

25259 7590 04/20/2004

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER

MEISLAHN, DOUGLAS J

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 04/20/2004

16

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/240,265

Applicant(s)

PETERS, MARK E.

Examiner

Douglas J. Meislahn

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 February 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-12 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-12 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 09 February 2004 that amended claims 1 and 7 and added claims 10-12.

Response to Arguments

2. Applicant's arguments filed 09 February 2004 have been fully considered but they are not persuasive. Sections A and B are identical to explanations and arguments filed in the amendment B, dated 17 July 2003. The examiner's responses to the relevant sections of amendment B are repeated below, in paragraphs 3-6.

3. Applicant partakes in a piecemeal analysis of the references, all the while generally remaining silent as to features of the present claims that are not shown by the cited prior art. The limitation that applicant does cite as being absent from the references is "extension", which applicant says is a term that has a known meaning within the art of X.509 certificates. While this is correct, the known meaning is not definite, as exhibited by Aucsmith et al.'s (6175626) and Sudia et al.'s (5995625) fifth figures, both of which show X.509 extensions. (Sudia et al.'s extension is made of elements 50 and 52.) Given the vagaries of what elements are necessarily part of an X.509 extension, the examiner has interpreted the word in its broadest, reasonable sense. As such, the bits in Shambroom that identify the cryptographic algorithms, which are additional information, read on an extension. The examiner recommends adding a clause to the independent claims that specifically lays out what applicant views as minimum requirements for an X.509 extension in the instant invention.

4. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

5. Applicant responds to the examiner's previous commentary on applicant's previous arguments. The first two paragraphs are discussed above. Applicant's third paragraph in this section returns to the subject of extension, which have been discussed above.

6. Applicant considers the motivation to combine Shear et al. with Shambroom to be less than compelling, partly because Shear et al. is not directed to certificates. The examiner is of the opinion that Shear et al., while specifically directed to load modules, executables, and other data elements, teaches multiple signatures created with dissimilar algorithms in a broadly applicable fashion, and thus the combination is proper. Furthermore, digital certificates are data elements, and hence Shear et al. is directly applicable thereto.

7. In the sentence bridging pages 8 and 9 of the response, applicant says that he "has never argued that the present invention claims the concept of using more than one algorithm for the purpose of security." In lines 6-7 of page 8, applicant says that the primary reference, Shambroom, does not show "multiple cryptographic algorithms employed by the certificate to protect its data, as per claim 1." Please clarify.

8. The first paragraph of section C is largely identical to a paragraph in the previous amendment. Its arguments have been refuted in the above.

9. The bits from Shambroom are the list. As shown above, an extension is too vaguely defined in the certificate art to have inherent limitations beyond those given by the plain English meaning of the word.

10. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., that the extensions are of an X.509 standard) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

11. The second full paragraph on page 10 is largely identical to the second full paragraph on page 9 of the previous response. Its arguments are rebutted above.

12. In response to applicant's argument that there is no suggestion to combine the references in the paragraph spanning pages 10 and 11, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, Shear et al. teach using multiple dissimilar digital signature algorithms to "reduce the scope of any specific compromise", a desirable outcome.

Applicant's arguments with respect to the applicability of Shear et al. have been discussed above.

13. Applicant's contention that the examiner erred in saying that "applicant agrees that the claims recite data" implies that applicant, in fact, does not believe that the claims recite data. A signature is data. As such, the claims clearly claim data. They do not, however, recite functional structure for the data. There is no interrelationship between elements, and so the data is not functionally related. Without specifying the details of an extension, the claimed material has no structure.

14. The previous office action, contrary to applicant's assertion, does not say that Shear et al. claim physical objects. The previous office action does not comment on the nature of Shear et al.'s claims.

15. Applicant's analysis of the combination of Shambroom and Schneier is inaccurate. With respect to claim 1, Schneier is used to explain elements of the X.509 certificate that is shown in Shambroom. The elements of the X.509 are inherent thereto and such inherent to Shambroom, even if they are not specifically taught by the reference. In this case, the references are combined in a manner similar to that of a two-reference 102, a valid, if rare, format. With respect to claim 2, Shambroom and Schneier are combined in the standard 103 format, noting features that are lacking in the primary reference (claim 2), support for these features in the secondary reference, and a "therefore" statement pertaining to their combination. The instant rejection also includes a motivation to combine, drawn from the secondary reference.

16. In the first paragraph of page 12, applicant's assessment of Shambroom ignores that the reference teaches X.509 certificates. As such there is no need for a motivation to combine X.509 certificates with Shambroom because they already exist in the reference. The motivation to combine Shear et al. with Shambroom is given above.

17. Applicant's arguments with respect to the applicability of the 101 rejection are unpersuasive because applicant's argument rests on mentioning claims in an unrelated case. No determination beyond the standard examination has been made with respect to Shear et al. If applicant believes that an error has been made in that determination, he is invited to contact the proper section within the patent office with a proper communiqué. The current response is not directed to the proper section of the patent office, nor does it invoke the reevaluation of a patent.

Claim Rejections - 35 USC § 101

18. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

19. Claims 1-3 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 1-3 claim data, which is nonfunctional descriptive material. As such, embodying the data on a computer-readable would NOT make the claims statutory. See MPEP 706.03(a) and, especially, 2106 IV B 1 (b).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

21. Claims 1-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Shambroom (5923756) and Schneier (*Applied Cryptography*) in view of Shear et al. (6157721).

In lines 32-35 of column 10, Shambroom discusses a certificate that includes a public key and list of one or more cryptographic algorithms supported by the entity associated with the public key. The certificate can resemble an X.509 certificate. On pages 574 and 575, Schneier describes the X.509 certificate. As can be seen in figure 24.2, the certificate includes a section that identifies the algorithm, parameters, and a public key. There is also a section for a signature. These read on the first clause of applicant's first claim. The list of algorithms disclosed in Shambroom also anticipates an extension for identifying at least one alternative algorithm. Shambroom does not dictate that a second public key and signature therefor be included in the certificate. In their abstract, Shear et al. say that using several dissimilar digital signature algorithms and their resultant signatures may "reduce the scope of any specific compromise." Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to put multiple signatures formed with different algorithms in Shambroom's exemplary X.509 certificate, thereby protecting the data from compromise. Inclusion of the secondary public key in the certificate would save an authenticator from tracking it down, thereby increasing efficiency.

With respect to claim 2, pages 480 and 481 of Schneier discuss elliptic curve public key systems. RSA is first mentioned on page 17. According to Schneier, it is the most popular public-key algorithm. There are trade-offs between the two, particularly in terms of the relative computational workloads of the two entities (signer and verifier). Therefore it would have been obvious to a person of ordinary skill in the art at the time the invention was made to support RSA and an elliptic curve cryptosystem with the X.509 certificate taught by Shambroom.

Both signatures verify at least part of the certificate and hence read on claim 3. Claims 4-6, 7-9, and 10-12 are largely the same as claims 1-3 and are rejected on the same grounds.

Conclusion


22. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Douglas J. Meislahn whose telephone number is (703) 305-1338. The examiner can normally be reached on between 9 AM and 6 PM, Monday through Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Douglas J. Meislahn
Examiner
Art Unit 2137

DJM